Alerta de seguridad cibernética	9VSA20-00310-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de octubre de 2020
Última revisión	22 de octubre de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de VMware referente a múltiples vulnerabilidades que afectan a los productos VMware ESXi, Workstation Pro/Player, Fusion Pro/Fusion, NSX-T y Cloud Foundation. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-3981
CVE-2020-3982
CVE-2020-3992
CVE-2020-3993
CVE-2020-3994
CVE-2020-3995

CVE-2020-3981

Debido a un problema en el control de acceso de archivos de sistema, es posible para un atacante sobrescribir ciertos archivos con privilegios de administrador a través de un ataque de enlace simbólico durante la instalación, causando una denegación de servicios en la máquina donde Horizon Client está instalado.

Productos Afectados

VMware ESXi versiones 7.0, 6.7 y 6.5.
VMware Cloud Foundation (ESXi) versiones 4.x y 3.x.

Mitigación

Para VMware ESXi, actualizar a la versión ESXi_7.0.1-0.0.16850804, ESXi670-202010401-SG o ESXi650-202010401-SG.
Para VMware Cloud Foundation (ESXi), actualizar a la versión 4.1 o 3.10.1.1.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0023.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3981

CVE-2020-3982

Debido a un problema en el control de acceso de archivos de sistema, es posible para un atacante sobrescribir ciertos archivos con privilegios de administrador a través de un ataque de enlace simbólico durante la instalación, causando una denegación de servicios en la máquina donde Horizon Client está instalado.

Productos Afectados

VMware ESXi versiones 7.0, 6.7 y 6.5.
VMware Cloud Foundation (NSX-T) versiones 4.x y 3.x.

Mitigación

Para VMware ESXi, actualizar a la versión ESXi_7.0.1-0.0.16850804, ESXi670-202010401-SG o ESXi650-202010401-SG.
Para VMware Cloud Foundation (NSX-T), actualizar a la versión 4.1 o 3.10.1.1.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0023.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3982

CVE-2020-3992

Debido a un problema en el control de acceso de archivos de sistema, es posible para un atacante sobrescribir ciertos archivos con privilegios de administrador a través de un ataque de enlace simbólico durante la instalación, causando una denegación de servicios en la máquina donde Horizon Client está instalado.

Productos Afectados

VMware ESXi versiones 7.0, 6.7 y 6.5.
VMware Cloud Foundation (ESXi) versiones 4.x y 3.x.

Mitigación

Para VMware ESXi, actualizar a la versión ESXi_7.0.1-0.0.16850804, ESXi670-202010401-SG o ESXi650-202010401-SG.
Para VMware Cloud Foundation (ESXi), actualizar a la versión 4.1 o 3.10.1.1.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0023.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3992

CVE-2020-3993

Debido a un problema en el control de acceso de archivos de sistema, es posible para un atacante sobrescribir ciertos archivos con privilegios de administrador a través de un ataque de enlace simbólico durante la instalación, causando una denegación de servicios en la máquina donde Horizon Client está instalado.

Productos Afectados

NSX-T versiones 3.x y 2.4.x.
VMware Cloud Foundation (NSX-T) versiones 4.x y 3.x.

Mitigación

Para NSX-T actualizar a la versión 3.0.2 o 2.5.2.2.0.
Para VMware Cloud Foundation (NSX-T), actualizar a la versión 4.1 o 3.10.1.1.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0023.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3993

CVE-2020-3994

Debido a un problema en el control de acceso de archivos de sistema, es posible para un atacante sobrescribir ciertos archivos con privilegios de administrador a través de un ataque de enlace simbólico durante la instalación, causando una denegación de servicios en la máquina donde Horizon Client está instalado.

Productos Afectados

VMware Horizon Client versión 5.x y anteriores para Windows.
VMware ESXi versiones 7.0, 6.7 y 6.5.
VMware Cloud Foundation (NSX-T) versiones 4.x y 3.x.

Mitigación

Actualizar a la versión 5.5.50 de VMware Horizon Client para Windows.
Para VMware ESXi, actualizar a la versión ESXi_7.0.1-0.0.16850804, ESXi670-202010401-SG o ESXi650-202010401-SG.
Para VMware Cloud Foundation (NSX-T), actualizar a la versión 4.1 o 3.10.1.1.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0023.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3994

CVE-2020-3995

Debido a un problema en el control de acceso de archivos de sistema, es posible para un atacante sobrescribir ciertos archivos con privilegios de administrador a través de un ataque de enlace simbólico durante la instalación, causando una denegación de servicios en la máquina donde Horizon Client está instalado.

Productos Afectados

VMware Horizon Client versión 5.x y anteriores para Windows.

Mitigación

Actualizar a la versión 5.5.50 de VMware Horizon Client para Windows.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0023.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3995